Objetivos del ENS

El Esquema Nacional de Seguridad establece la política de seguridad en la utilización de medios electrónicos por las Administraciones públicas y está constituido por un conjunto de principios básicos y requisitos mínimos que permiten una protección adecuada de la información. En este artículo se presenta esta importante herramienta normativa, con especial hincapié en los objetivos por ella perseguidos y en los aspectos más relevantes de su contenido.

POR MIGUEL ÁLVAREZ

El ENS está regulado por el Real Decreto 3/2010, de 8 de enero, y responde a la previsión que realiza el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

El Esquema se ha obtenido como resultado de un proceso coordinado por el Ministerio de la Presidencia, con el apoyo del Centro Criptológico Nacional (CCN), en el que han participado todas las Administraciones públicas, a través de los órganos colegiados con competencia en materia de Administración electrónica. Más de un centenar de expertos de las Administraciones Públicas han colaborado en su elaboración a lo largo de los últimos tres años; a los que hay que sumar los numerosos expertos que también han aportado su opinión a través de las asociaciones profesionales de la industria del sector TIC. Todo ello a la luz del estado del arte y de los principales referentes en materia de seguridad de la información.

El mandato esencial del ENS es que todos los órganos superiores de las administraciones públicas deberán disponer de su política de seguridad que garantice el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos.

El ENS tiene los objetivos siguientes:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes, a través de estos medios.

Introducir los elementos comunes que han de guiar la actuación de las administraciones públicas en materia de seguridad de las tecnologías de la información.

- Aportar un lenguaje común para facilitar la interacción de las administraciones públicas, así como la comunicación de los requisitos de seguri-

dad de la información a la Industria.

El contenido principal del ENS incluye lo siguiente:

•Los principios básicos a ser tenidos en cuenta en las decisiones en materia de seguridad.

•Los requisitos mínimos que permitan una protección adecuada de la información.

•La categorización de los sistemas para la adopción de medidas de seguridad proporcionadas a la naturaleza de la información, del sistema y de los servicios a proteger, y a los riesgos a los que están expuestos. Para facilitar la aplicación del principio de proporcionalidad se contempla la categorización de los sistemas en tres escalones, en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios, con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, atendiendo a la repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio y el respeto de la legalidad y de los derechos de los ciudadanos.

•Hecha esta valoración, la selección de las medidas de seguridad apropiadas se ha de realizar de acuerdo con las dimensiones de seguridad y sus niveles y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema. Se contemplan medidas de seguridad relacionadas con la organización global de la seguridad, con la protección de la operación del sistema como conjunto integral de componentes para un fin, y con la protección de activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

•La auditoría de la seguridad que verifique el cumplimiento del ENS, al menos cada dos años en el caso de los sistemas de categorías Media y Alta. En este punto se sigue el modelo aplicado a la protección de datos de carácter personal en el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD.

•La respuesta a incidentes de seguridad, mediante la estructura CCN-CERT, que actuará sin perjuicio de las capacidades de respuesta que pueda tener cada administración pública, y de su función como coordinador a nivel nacional e internacional, prestando los servicios de soporte y coordinación, investigación y divulgación, formación e información.

•La certificación como aspecto a considerar al adquirir productos de seguridad, citando al Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC (el propio Centro Criptológico Nacional).

Para lograr un mejor cumplimiento del Esquema se hace referencia a la utilización de los servicios e infraestructuras comunes y a las guías de seguridad de las TIC, las cuales elaborará y difundirá el Centro Criptológico Nacional.

Adicionalmente se tratan otros aspectos tales como los que se indican a continuación:

•Se recogen las condiciones técnicas de seguridad de las comunicaciones electrónicas, así como los requerimientos técnicos de notificaciones y publicaciones electrónicas y firma electrónica.

•Se encomienda al Comité Sectorial de Administración Electrónica que articule los procedimientos necesarios para conocer regularmente el estado de las principales variables la seguridad en los sistemas de información a los que se refiere el real decreto.

•Se tratan también las normas de conformidad con el ENS en cuanto a sedes y registros electrónicos; la inclusión de las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas; los mecanismos de control para garantizar el cumplimiento del Esquema; así como la publicidad en las sedes electrónicas de las declaraciones de conformidad y de los distintivos de seguridad, obtenidos respecto al cumplimiento del Esquema.

•Las disposiciones adicionales inciden en cuestiones relativas a: la formación necesaria para garantizar el conocimiento del ENS por parte del personal de las Administraciones públicas; a INTECO y otras entidades análogas, que podrán desarrollar proyectos de innovación y programas de investigación dirigidos a la mejor implantación de las medidas de seguridad contempladas en el Esquema; y al establecimiento de un órgano colegiado para la cooperación de las Administraciones públicas en materia de adecuación e implantación de lo previsto en el Esquema.

Finalmente, se articula un mecanismo escalonado para la adecuación a lo previsto en el ENS, de forma que los sistemas existentes se deberán adecuar al Esquema en 12 meses, aunque, si hubiese circunstancias que impidan la plena aplicación, se dispondrá de un plan de adecuación que marque los plazos de ejecución, en ningún caso superiores a 48 meses desde la entrada en vigor del Esquema.

Miguel Álvarez
Jefe del Área de Cooperación en TI
D.G. Impulso Administración Electrónica
Ministerio de la Presidencia